CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

May 25, 2007

S. 239
Notification of Risk to Personal Data Act of 2007

As ordered reported by the Senate Committee on the Judiciary on May 3, 2007

SUMMARY

S. 239 would require most government and business entities that collect, transmit, store, or use personal information to notify individuals whose information has been unlawfully accessed through a security breach. The legislation defines sensitive personal information as combinations of an individual's name, address or phone number, and Social Security number, driver's license number, financial account information, or biometric data (i.e., finger print, voice print, or retina scan). Under certain circumstances, entities could apply to the Secret Service for exemptions from the notification requirements. In addition, S. 239 would create civil penalties for entities that fail to provide notice to affected individuals.

Implementing S. 239 could increase collections of civil penalties that would affect revenues, but CBO estimates that any such effect would not be significant in any year. In addition, enacting S. 239 could affect direct spending by agencies not funded through annual appropriations for the notification requirements. CBO estimates, however, that any changes in net spending by those agencies would be negligible. Complying with the bill's provisions could increase the expenses of the Secret Service, but CBO estimates that such costs would be less than $500,000 annually and subject to the availability of appropriated funds.

S. 239 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that the cost of complying with the requirements would be small and would not exceed the threshold established in UMRA ($66 million in 2007, adjusted annually for inflation).

S. 239 also contains private-sector mandates as defined in UMRA. The bill would require entities engaged in interstate commerce to notify individuals and other entities outlined in the bill if a security breach occurs in which such individuals' sensitive personally identifiable information is compromised. In addition, the bill would require consumer reporting agencies to include a fraud alert in a consumer's file if that consumer submits evidence that they have received notice regarding their financial information being compromised.

Because of the uncertainty about the number of entities that are already in compliance with the notification requirements in the bill, CBO cannot estimate the incremental cost of complying with those mandates. Consequently, CBO cannot determine whether the direct cost of the mandates in the bill would exceed the annual threshold established by UMRA for private-sector mandates ($131 million in 2007, adjusted annually for inflation).

ESTIMATED COST TO THE FEDERAL GOVERNMENT

In the event of a security breach, S. 239 would require most government agencies to notify individuals whose personal information has been unlawfully accessed. Notification would be in the form of individual notice (written notice to a home mailing address, telephone call, or via e-mail) as well as through the mass media for breaches exceeding 5,000 individuals. The legislation also would require the agency to provide affected individuals with a description of the accessed information, a toll-free number to contact the agency, the names and toll-free telephone numbers of the major credit-reporting agencies, and in some instances, information on an individual state's victim assistance protection.

This provision would codify the current practice of the federal government regarding security breach notification. While existing laws generally do not require agencies to notify affected individuals of data breaches this has been the practice of agencies that have experienced security breaches. Therefore, CBO expects that implementing those notification provisions would probably not lead to a significant increase in spending. Nonetheless, the federal government is also one of the largest providers, collectors, consumers, and disseminators of personnel information in the United States. Although, CBO cannot anticipate the number of security breaches, a significant breach of security involving a major collector of personnel information, such as the Internal Revenue Service or the Social Security Administration, could involve millions of individuals, and there would be significant costs to notify individuals of such a security breach.

Enacting S. 239 could affect both direct spending and revenues, but CBO estimates that any such effects would be negligible.

IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

S. 239 contains intergovernmental mandates as defined in UMRA. Specifically, the bill would explicitly preempt state laws in at least 35 states regarding the treatment of personal information and place certain notification requirements and limitations on state Attorneys General and state insurance authorities. CBO estimates that the cost of complying with the requirements would be small and would not exceed the threshold established in UMRA ($66 million in 2007, adjusted annually for inflation).

IMPACT ON THE PRIVATE SECTOR

S. 239 contains private-sector mandates as defined in UMRA. The bill would require entities engaged in interstate commerce to notify individuals and other entities outlined in the bill if a security breach occurs in which such individuals' sensitive personally identifiable information is compromised. In addition, the bill would require consumer reporting agencies to include a fraud alert in a consumer's file if that consumer submits evidence that they have received notice regarding their financial information being compromised.

Because of the uncertainty about the number of entities that are already in compliance with the notification requirements in the bill, CBO cannot estimate the incremental cost of complying with those mandates. Consequently, CBO cannot determine whether the direct cost of the mandates in the bill would exceed the annual threshold established by UMRA for private-sector mandates ($131million in 2007, adjusted annually for inflation).

Security Breach Notification

S. 239 would require business entities engaged in interstate commerce that use, access, transmit, store, or dispose of or collect sensitive personally identifiable information, following the discovery of a security breach, to notify any U.S. resident whose information may have been accessed or acquired and results in a risk of harm to such individuals. Entities would be able to notify individuals using written letters, telephone, or e-mail under certain circumstances. The bill also would require those entities to notify the owner or license of any such information that the entity does not own or license but would exempt business entities from those requirements under certain circumstances.

Business entities would be required to notify consumer reporting agencies, certain major media outlets, or the Secret Service in the event of a large security breach as outlined in the bill.

The cost of the mandates would depend on the number of security breaches that occur. According to industry and government sources, millions of individuals' sensitive personally identifiable information is illegally accessed every year. However, according to those sources, 38 states already have laws requiring notification in the event of a security breach. In addition, it is the current practice of many business entities to notify individuals in the event of a security breach and many business entities utilize security programs that would exempt them from the notification requirements in this bill. Because of uncertainty about the number of entities that are already in compliance with the notification mandates, CBO cannot estimate the incremental cost of complying with the notification requirements under the bill.

Fraud Alert

The bill also would require consumer reporting agencies to include an extended fraud alert in a consumer's file if that consumer submits evidence that they have received notice that the consumer's financial information has or may have been compromised. Under current law, consumer reporting agencies are required to provide a extended fraud alert service if a consumer submits an identity theft report and a temporary fraud alert if requested by a consumer in good faith. The cost of the mandate would be the incremental cost for consumer reporting agencies to include additional extended fraud alerts in consumers' files. Based on information from industry sources, CBO estimates that the incremental cost to comply with this mandate would be minimal.

PREVIOUS CBO ESTIMATE

On May 17, 2007, CBO transmitted a cost estimate for S. 495, the Personal Data Privacy and Security Act of 2007, as ordered reported by the Senate Committee on the Judiciary on May 3, 2007. The two bills are both concerned with security breaches and notification requirements for the federal government and private industry. S. 495 would require the Federal Trade Commission to increase its efforts to assist victims of identity theft and authorize other activities. CBO estimated that implementing S. 495 would cost $335 million over the 2007-2012 period. CBO has determined that both bills contain intergovernmental and private-sector mandates. In both cases, we estimate that the cost of the intergovernmental mandates would not exceed the threshold established in UMRA ($66 million in 2007, adjusted annually for inflation). CBO cannot estimate the cost of the private-sector mandates in the two bills.

ESTIMATE PREPARED BY:

Federal Costs: Matthew Pickford and Mark Grabowicz
Impact on State, Local, and Tribal Governments: Elizabeth Cove
Impact on the Private Sector: Paige Piper/Bach

ESTIMATE APPROVED BY:

Peter H. Fontaine
Deputy Assistant Director for Budget Analysis